REMARKS

Claims 1-24 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 101

The Examiner rejected Claims 1-22 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. This rejection is respectfully traversed.

Applicants respond to the Claim 1 rejection be showing that such claim has previously been amended to specifically recite a data processing apparatus-implemented method, and that the recited steps are data processing apparatus-implemented steps. Thus, amended Claim 1 is shown to expressly recite technology and therefore is directed to "useful arts".

Applicants respond to the Claim 12 rejection by showing that, and contrary to the Examiner's assertion, such claim does *not* claim a method. Rather, Claim 12 expressly recites an *apparatus* with corresponding "means for" elements, as shown below:

> 12. An **apparatus** for creating a privacy policy, comprising:
> creation **means for creating** a policy group;
> movement **means for moving** a data element to the policy group; and
> generation **means for generating** a privacy policy based on the policy group.

Per 35 USC 112, 6th paragraph, "means for" elements shall be construed to cover the corresponding structure or material described in the specification and equivalents thereof. Thus, the recited means for elements are shown to not merely describe a process that might be performed without the aid of any technology, as alleged by the Examiner, and Claim 12 is thus shown to have been erroneously rejected under 35 USC 101.

In response to this amendment and argument, the Examiner states in the final rejection of these claims, on page 3 in the "Response to Arguments" section:

> "In the present application claims 1 and 12 only recites an abstract idea. In claims 1 and 12 the applicant claims a method for creating policy

> groups, moving a data element between groups and generating a privacy policy based upon the policy group. *This process might be performed without the aid of any technology* and therefore the claimed method is not within the technological arts." (emphasis added by Applicants)

Applicants show error in such assertion, as Claim 1 was previously amended to expressly recited the technological aid for which the Examiner continues to maintain is lacking. In particular, Claim 1 expressly recites "data processing apparatus-implemented steps of: creating a policy group; moving a data element to the policy group; and generating a privacy policy based on the policy group". Thus, Claim 1 is not a mere abstract idea that might be performed without the aid of any technology, but expressly recites steps performed with the aid of technology, and in particular expressly recites steps performed by a data processing system apparatus (i.e. technology). Thus, Claim 1 is not a mere abstract idea, and therefore Claim 1 is shown to have been erroneously rejected under 35 U.S.C. 101.

Further regarding Claim 12, in the detailed rejection of such claim under 35 USC 101 in the present final office action, the Examiner states:

> "In claims 1 **and 12** the applicant claims a **method** for creating policy groups, moving a data element between groups and generating a privacy policy based upon the policy group. This process might be performed without the aid of any technology and therefore **the claimed method** is not within the technological arts." (emphasis added by Applicants)

Claim 12 has been reproduced above in its entirely, and Applicants urge that – contrary to the Examiner's assertion regarding Claim 12 in making the rejection of Claims 12 final under 35 USC 101 – Claim 12 is not directed to a method, but rather to an apparatus. Thus, the Examiner's reasoning regarding Claim 12 in finally rejecting such claim under 35 USC 101 is shown to be clear error, as such claim does not merely recite a method or an abstract idea, as alleged by the Examiner, but rather explicitly recites an apparatus.

With respect to dependent Claims 2-11 and 13-22, Applicants traverse for reasons given above regarding their respective independent claims.

Thus, the rejection of Claims 1-22 under 35 U.S.C. § 101 has been overcome.

II. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 1-24 under 35 U.S.C. § 103 as being unpatentable over Moriconi et al (US Patent 6,158,010) in view of Abraham et al. (WO 98/40987). This rejection is respectfully traversed.

In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id. To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974) (emphasis added by Applicants). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Applicants will now show that all of the claim limitations are not taught or suggested by the cited references.

A. Generally speaking, the present invention is directed to *privacy policies*, and in particular to methods and apparatus for creating a *privacy policy*. None of the cited references teach or suggest any type of privacy policy, or the creation of a privacy policy.

Specifically with respect to Claim 1, such claim recites a data processing apparatus-implemented method for creating a *privacy policy*. In contrast, the teachings in the cited Moriconi reference are directed to ensuring that clients are authorized to access securable components (Col. 13, lines 14-32) by use of a security policy (Claim 1). Security and privacy are two very different concepts, and the teaching of one (security, as taught by Moriconi) does not teach or suggest the other (privacy, as claimed). For example, imagine a person living in a locked, bullet-proof glass house, where the glass is see-through. This locked, bullet-proof glass house is certainly secure, but it is not at all private. As another example, assume that an ID is required to authenticate that a user is who they are in order to receive a ballot for voting. However, the ballot itself has the user's name/identifier on it. The user has been authorized to vote, but the voting is certainly not private as the voter's name is in the ballot. Thus, authorization and privacy are very different concepts, as will now be further described (with supporting evidence).

The following is an excerpt from a document entitled "Authorization and Privacy for Semantic Web Services", published by IEEE Distributed Online Systems, which is from the July/Aug 2004 issue of IEEE Intelligent systems. The document, which is attached hereto in Appendix A, was found by Applicants on the internet at http://dsonline.computer.org/0410/f/x4kag.htm. The document clearly shows that authorization policies and privacy policies are not the same, and that one is not a subset of the other. They are different. Applicants urge that a teaching of authorization – as taught by the cited Moriconi reference - does not teach or suggest any type of privacy policy, as claimed.

Role of policies

Policies specify who can use a service and under which conditions, how information should be provided to the service, and how the provided information will be used. Policies should be part of Web Service representations—particularly those on the Semantic Web (see the "Related Work" sidebar for more background information).

In our work, a client-server model involves a client that wants to invoke a Web Service. We view the use of policies as *symmetric*—policies that constrain both the provider and requester. You can easily extend this model to a service-service architectural model.

Here, we address two kinds of policies: *privacy* and *authorization*. Privacy policies specify under what conditions you can exchange information and the legitimate uses of that information. For example, a privacy policy might say that a provider could give a requester a key to access private information only if the key is encrypted during transmission. When a requester discovers the policy, it should decide whether it can satisfy this condition. The requester might have its own privacy policy that requires keeping certain information confidential, so it likewise can't share unencrypted private information. The requestor's privacy policy prevents it from interacting with Web Services that don't perform the needed encryption.

Privacy policies help specify data confidentiality during transmission as well as after receipt. Consider a service that says it won't distribute details it receives as input. A requester that values privacy might see this as an important requirement.

You can interpret a Web Service's privacy policies as an obligation and contract. For example, if after invocation, a service does provide a requester's details to a telemarketer, the person represented by the requester could take legal action against the service on the basis of the policy. As financial transactions become more common among Web Services and as Web Services start dealing with confidential information (such as names,

> addresses, social security numbers (SSNs), credit cards, and telephone numbers), more people will expect the enforcement of privacy policies.
>
> Authorization policies constrain the provider to accept requests for service only from certain clients. For example, a service's authorization policy could state that a requester must act on behalf of a person who belongs to a certain organizational group and can prove membership with a digital certificate. Similarly, the requester could limit invocation to selected providers.

Also attached hereto in Appendix B is a datasheet from Electronic Data Systems Corporation (EDS) regarding their Security and Privacy Consulting Services. If security and privacy were coextensive, or even if one were a subset of the other, there would be no reason to include both terms in the title of this document as it would be redundant. Because each term is used in the title further evidences that one does not mean, or otherwise include/cover, the other.

Thus, per the technological arts, authorization/security policies and privacy policies are different, and a teaching of one does not teach or suggest the other.

Even in the non-technological arts, it is commonly known that in today's environment with terrorists-related concerns, people everywhere are having to make trade-offs regarding their own privacy in the name of security (as shown in Appendix C in a document entitled "Trading Privacy for Security Without a Thought", by Ellen Goodman and posted at www.siliconvalley.com on Oct. 6, 2002). This further evidences that these terms (security and privacy) mean different things to those of ordinary skill in the art.

Therefore, it is shown that the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 1.

B. The Examiner takes the position that an authorization policy "by definition" is also enforcing a privacy policy. Applicants show two-fold error in such assertion. First, an authorization policy does *not*, by definition, also enforce a privacy policy. The Examiner provides no evidence whatsoever to substantiate such assertion, but rather makes a single sentence unsubstantiated assertion. Applicants have provided evidence (above) that an authorization policy is different from a privacy policy, and therefore an authorization policy does not, by definition, also enforce a privacy policy.

Even assuming arguendo that an authorization policy does also enforce a privacy policy (which Applicants urge it does not), Claim 1 is not merely directed to *enforcement* of a privacy policy. Rather, Claim 1 is directed to the *establishment* of a privacy policy. By analogy, legislatures make laws which the police enforce. Enforcement of laws (by the police) is very different from the process of establishing laws (by legislatures). Similarly, the Examiner's position that a teaching of an authorization policy "by definition" also *enforces* a privacy policy does not establish any teaching or suggestion of any step, process or method for *creating* a privacy policy, as expressly recited in Claim 1. Therefore, even assuming arguendo that the Examiner's assertion regarding authorization and privacy is true (which Applicants urge it is not), the Examiner has still failed to establish a prima facie showing of obviousness as the Examiner has failed to establish any teaching or suggestion of *creating* a privacy policy, or any step of *creating* a privacy policy based on a policy group. Thus, Claim 1 is further shown to have been erroneously rejected Claim 1 under 35 USC 103.

C. Quite simply, a teaching of a creating an authorization/security policy does not teach or otherwise suggest any type of privacy policy, and in particular does not teach or suggest a method for creating a privacy policy, as expressly recited in Claim 1. A prima facie case of obviousness has therefore not been established by the Examiner with respect to Claim 1, and therefore Claim 1 is shown to have been erroneously rejected.

Applicants traverse the rejection of Claims 2-11 for reasons given above with respect to Claim 1 (of which Claims 2-11 depend upon).

Applicants traverse the rejection of Claims 12-24 for similar reasons to those given above with respect to Claim 1.

Therefore, the rejection of Claims 1-24 under 35 U.S.C. § 103 has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 11/2/05

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.